MODULAR REPRESENTATIONS ARISING FROM SELF-DUAL ℓ-ADIC REPRESENTATIONS OF FINITE GROUPS

ALICE SILVERBERG AND YURI ZARHIN

Let G be a finite subgroup of a symplectic group $\mathrm{Sp}_{2d}(\mathbf{Q}_\ell)$. Despite the fact ([3]) that G can fail to be conjugate in $\mathrm{GL}_{2d}(\mathbf{Q}_\ell)$ to a subgroup of $\mathrm{Sp}_{2d}(\mathbf{Z}_\ell)$, we prove that it can nevertheless be embedded in $\mathrm{Sp}_{2d}(\mathbf{F}_\ell)$ in such a way that the characteristic polynomials are preserved (mod ℓ), as long as $\ell > 3$.

We start with the following "rigidity" result, which is in the spirit of similar results by Minkowski and Serre.

Proposition 1. *Suppose ℓ is a prime number, and K is a discrete valuation field of characteristic zero and residue characteristic ℓ. Let $\mathcal{O}$ denote the valuation ring and λ the maximal ideal. Let e denote the ramification index of K (i.e., $\ell\mathcal{O} = \lambda^e$), and suppose $2e < \ell - 1$. Suppose S is a free $\mathcal{O}$-module of finite rank, A is an automorphism of S of finite order, and $(A-1)^2 \in \lambda\mathrm{End}(S)$. Then $A = 1$.*

Proof. This follows directly from Theorem 6.2 of [2] with $n = \ell$ and $k = 2e$. □

Note that the hypothesis $2e < \ell - 1$ is satisfied if $e = 1$ and $\ell \geq 5$. Next we state our main theorem.

Theorem 2. *Suppose ℓ is a prime number, and K is a discrete valuation field of characteristic zero and residue characteristic ℓ. Let $\mathcal{O}$ denote the valuation ring, let λ denote its maximal ideal, and let k denote the residue field $\mathcal{O}/\lambda$. Let e denote the ramification index of K, and suppose $2e < \ell - 1$. Suppose V is a K-vector space of finite dimension N, suppose $f : V \times V \to K$ is a nondegenerate alternating (respectively, symmetric) K-bilinear form, suppose G is a finite group, and suppose*

$$\rho : G \hookrightarrow \mathrm{Aut}_K(V, f)$$

is a faithful representation of G on V that preserves the form f. Then there exist a nondegenerate alternating (respectively, symmetric) k-valued k-bilinear form f_0 on k^N, and a faithful representation

$$\bar{\rho} : G \hookrightarrow \mathrm{Aut}_k(k^N, f_0),$$

such that for every $g \in G$, the characteristic polynomial of $\bar{\rho}(g)$ is the reduction modulo λ of the characteristic polynomial of $\rho(g)$.

Proof. If S is a G-stable $\mathcal{O}$-lattice in V, let

$$S^* = \{x \in V : f(x, S) \subseteq \mathcal{O}\}.$$

Fix a G-stable $\mathcal{O}$-lattice S in V. Let π denote a uniformizer for $\mathcal{O}$. Multiplying f by an integral power of π if necessary, we may assume that $f(S, S) = \mathcal{O}$. Then $S \subseteq S^*$. Let $S_0 = S$ and let

$$S_{i+1} = S_i + (\pi^{-1} S_i \cap \pi S_i^*) \quad \text{for} \quad i \geq 0.$$

Silverberg would like to thank NSA, NSF, and the Science Scholars Fellowship Program at the Bunting Institute for financial support. Zarhin would like to thank NSF for financial support.

Then S_i is a G-stable $\mathcal{O}$-lattice in V, $f(S_i, S_i) = \mathcal{O}$, and $S_i \subseteq S_{i+1} \subseteq S_{i+1}^* \subseteq S_i^*$. Note that $S_{i+1} = S_i$ if and only if $\pi S_i^* \subseteq S_i$. We have

$$S = S_0 \subseteq S_1 \subseteq S_2 \subseteq \ldots \subseteq S^*.$$

Since S^*/S is finite, we have $S_j = S_{j+1}$ for some j. Let $T = S_j$. Then T is a G-stable $\mathcal{O}$-lattice in V such that $f(T,T) = \mathcal{O}$ and $\lambda T^* = \pi T^* \subseteq T$.

Let $\bar{f} : T/\lambda T \times T/\lambda T \to k$ be the reduction of f modulo λ. Then $\ker(\bar{f}) = \lambda T^*/\lambda T \cong T^*/T$. Clearly, $\bar{f}$ is nondegenerate on $(T/\lambda T)/\ker(\bar{f}) \cong T/\lambda T^*$. On $T^* \times T^*$, the form πf is $\mathcal{O}$-valued. Let $\tilde{f}$ denote the reduction modulo λ of the restriction of πf to $T^* \times T^*$. Since $(T^*)^* = T$, we have $\ker(\tilde{f}) = T/\lambda T^*$. Therefore, $\tilde{f}$ is nondegenerate on $(T^*/\lambda T^*)/(T/\lambda T^*) \cong T^*/T \cong \ker(\bar{f})$. We thus obtain a homomorphism

$$\psi : G \to \mathrm{Aut}_k((T/\lambda T)/\ker(\bar{f}), \bar{f}) \times \mathrm{Aut}_k(\ker(\bar{f}), \tilde{f}) \cong$$

$$\mathrm{Aut}_k(T/\lambda T^*, \bar{f}) \times \mathrm{Aut}_k(T^*/T, \tilde{f}) \hookrightarrow \mathrm{Aut}_k(T^*/\lambda T^*, \bar{f} \times \tilde{f}) \cong \mathrm{Aut}_k(k^N, f_0)$$

for an appropriate pairing f_0. All the elements $\sigma \in \ker(\psi)$ act as the identity on $T/\lambda T^*$ and on T^*/T, and thus $(\sigma - 1)^2 T^* \subseteq \lambda T^*$. Proposition 1 implies ψ is injective. Let $\bar{\rho} = \psi$. □

Remark 3. If one is concerned only with preserving the characteristic polynomials, and does not insist that $\bar{\rho}$ be an embedding, then in the symplectic case the above result can instead be achieved with the aid of Proposition 8 of [1], rather than Proposition 1 above.

Theorem 4. *Suppose ℓ is a prime number, and L is a discrete valuation field of characteristic zero and residue characteristic ℓ. Suppose K is a quadratic extension of L, let $\mathcal{O}$ denote its valuation ring, let λ denote the maximal ideal, and let $k = \mathcal{O}/\lambda$. Let e denote the ramification index of K, and suppose $2e < \ell - 1$. Suppose V is a K-vector space of finite dimension N, suppose $f : V \times V \to K$ is a nondegenerate pairing which is hermitian (respectively, skew-hermitian) with respect to the extension K/L, suppose G is a finite group, and suppose $\rho : G \hookrightarrow \mathrm{Aut}_K(V, f)$ is a faithful representation. Suppose K/L is unramified and thus k is a quadratic extension of the residue field k_L of L. Then there exist a nondegenerate k-valued pairing f_0 on k^N which is hermitian (respectively, skew-hermitian) with respect to the extension k/k_L, and a faithful representation $\bar{\rho} : G \hookrightarrow \mathrm{Aut}_k(k^N, f_0)$, such that for every $g \in G$, the characteristic polynomial of $\bar{\rho}(g)$ is the reduction modulo λ of the characteristic polynomial of $\rho(g)$.*

Proof. Let π denote a uniformizer for L. Then π is also a uniformizer for K, and the proof is a repetition of the proof of Theorem 2. The reductions $\bar{f}$ and $\tilde{f}$ are now hermitian (respectively, skew-hermitian). □

Remark 5. In the setting of Theorem 4, suppose now that K/L is ramified. Then $k_L = k$, and one can write $K = L(\sqrt{D})$ where D is a uniformizer for L and $\pi = \sqrt{D}$ is a uniformizer for K. Let S be a G-stable $\mathcal{O}$-lattice in V. Then $\pi^r f(S,S) = \mathcal{O}$ for some integer r. If r is even then $\pi^r f$ is hermitian (respectively, skew-hermitian) and its reduction is symmetric (respectively, alternating). Further, $\pi^{r+1} f$ is skew-hermitian (respectively, hermitian) and its reduction is alternating (respectively, symmetric). If r is odd, then $\pi^r f$ is skew-hermitian (respectively, hermitian) and

its reduction is alternating (respectively, symmetric). Further, $\pi^{r+1}f$ is hermitian (respectively, skew-hermitian) and its reduction is symmetric (respectively, alternating). In all cases one can proceed as in Theorem 2 and obtain an embedding of G into a product of an orthogonal group $\mathrm{O}_s(k)$ and a symplectic group $\mathrm{Sp}_{n-s}(k)$, which "respects" the characteristic polynomials.

Lemma 6. *Suppose F is a field of characteristic not equal to 2 and $f : F^2 \times F^2 \to F$ is a nondegenerate symmetric pairing. Let $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(F)$. Then f is not g-invariant.*

Proof. Let $\{u, v\}$ denote the standard basis of F^2 over F. Suppose f is g-invariant. Then $f(u, v) = f(gu, gv) = f(u, u+v)$, i.e., $f(u, u) = 0$. Also, $f(v, v) = f(gv, gv) = f(u + v, u + v) = f(v, v) + 2f(u, v)$, since f is symmetric. Since $\mathrm{char}(F) \neq 2$, we have $f(u, v) = 0$. Therefore $f(u, w) = 0$ for every $w \in F^2$, contradicting the nondegeneracy of f. $\square$

Let Q_8 denote the quaternion group of order 8. Let ζ_ℓ denote a primitive ℓ-th root of unity. The next two results show that the condition $2e < \ell - 1$ in Theorem 2 is sharp, in both the symmetric and alternating cases.

Proposition 7. *Let ℓ be an odd prime number, let $K = \mathbf{Q}_\ell(\zeta_\ell + \zeta_\ell^{-1})$, let V be $\mathbf{Q}_\ell(\zeta_\ell)$ viewed as a 2-dimensional K-vector space, and let $G = \boldsymbol{\mu}_\ell$. Then there exists a nondegenerate symmetric K-bilinear form $f : V \times V \to K$ such that there is a faithful irreducible representation $G \hookrightarrow \mathrm{Aut}_K(V, f)$. However, if F is a field of characteristic ℓ (in particular, if $F = \mathbf{F}_\ell$), then there does not exist a nondegenerate symmetric F-bilinear form $f_0 : F^2 \times F^2 \to F$ such that G embeds in $\mathrm{Aut}_F(F^2, f_0)$.*

Proof. Let $M = \mathbf{Q}_\ell(\zeta_\ell)$, and let $x \mapsto \bar{x}$ denote the nontrivial automorphism of M over K. Define f by $f(x, y) = \mathrm{tr}_{M/K}(x\bar{y})$. The desired injection is given by sending ζ_ℓ to multiplication by ζ_ℓ. The nonexistence of f_0 follows from Lemma 6, since if g is an element of $\mathrm{GL}_2(F)$ of order ℓ, then there exists a basis of F^2 with respect to which $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. $\square$

Proposition 8. *Let ℓ be an odd prime number, let $K = \mathbf{Q}_\ell(\zeta_\ell + \zeta_\ell^{-1})$, let V be $\mathbf{Q}_\ell(\zeta_\ell)^2$ viewed as a 4-dimensional K-vector space, and let $G = Q_8 \times \boldsymbol{\mu}_\ell$. Then there exist a nondegenerate alternating K-bilinear form $f : V \times V \to K$ and a faithful irreducible representation $\rho : G \hookrightarrow \mathrm{Aut}_K(V, f)$ such that there do not exist a field F of characteristic ℓ, a nondegenerate alternating F-valued F-bilinear form f_0 on F^4, and a faithful representation $\bar{\rho} : G \hookrightarrow \mathrm{Aut}_F(F^4, f_0)$, having the property that for every $g \in G$, the characteristic polynomial of $\bar{\rho}(g)$ is the reduction of the characteristic polynomial of $\rho(g)$.*

Proof. Let $M = \mathbf{Q}_\ell(\zeta_\ell)$, let $x \mapsto \bar{x}$ denote the nontrivial automorphism of M over K, and let V_2 be M viewed as a 2-dimensional K-vector space. Then $V = V_2 \times V_2 = \mathbf{Q}_\ell^2 \otimes_{\mathbf{Q}_\ell} V_2$. Let D_2 denote the quaternion algebra over $\mathbf{Q}$ ramified exactly at 2 and infinity. Then Q_8 is a subgroup of $D_2^\times$. The isomorphism $D_2 \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \cong \mathrm{M}_2(\mathbf{Q}_\ell)$ induces a natural, absolutely irreducible, faithful representation $\rho_1 : Q_8 \hookrightarrow \mathrm{SL}_2(\mathbf{Q}_\ell) \cong \mathrm{Aut}(\mathbf{Q}_\ell^2, f_1)$ where f_1 is the standard alternating pairing on $\mathbf{Q}_\ell^2$. The natural action of $\boldsymbol{\mu}_\ell$ on V_2 respects the nondegenerate symmetric bilinear form

$f_2 : V_2 \times V_2 \to K$ defined by $f_2(x,y) = \mathrm{tr}_{M/K}(x\bar{y})$. We thus obtain a faithful representation $\rho_2 : \boldsymbol{\mu}_\ell \hookrightarrow \mathrm{Aut}_K(V_2, f_2)$. Let ρ be the representation

$$\rho : G = Q_8 \times \boldsymbol{\mu}_\ell \hookrightarrow \mathrm{SL}_2(\mathbf{Q}_\ell) \times \mathrm{Aut}_K(V_2, f_2) \hookrightarrow \mathrm{Aut}_K(V, f)$$

defined by $\rho(a,b) = \rho_1(a) \otimes \rho_2(b)$, where $f = f_1 \otimes f_2$. For every element $\sigma \in Q_8 \subset G$ of order 4, the characteristic polynomial of $\rho(\sigma)$ is $(t^2+1)^2$. For the element $-1 \in Q_8 \subset G$ of order 2, the characteristic polynomial of $\rho(-1)$ is $(t+1)^4$.

Suppose there exist a field F of characteristic ℓ, a nondegenerate F-valued alternating pairing f_0 on F^4, and a faithful representation $\bar{\rho} : G \hookrightarrow \mathrm{Aut}_F(F^4, f_0)$ such that the characteristic polynomial of $\bar{\rho}(\sigma)$ is $(t^2+1)^2$ for every $\sigma \in Q_8$ of order 4 and the characteristic polynomial of $\bar{\rho}(-1)$ is $(t+1)^4$. Let V_0 denote the corresponding faithful symplectic $F[G]$-module. Since $\#Q_8$ is not divisible by ℓ, V_0 is a semisimple $F[Q_8]$-module. By choosing a suitable basis we may assume that $\rho_1(Q_8) \subset \mathrm{SL}_2(\mathbf{Z}_\ell)$. The composition of ρ_1 with the reduction map gives a faithful representation $\bar{\rho}_1 : Q_8 \hookrightarrow \mathrm{SL}_2(\mathbf{F}_\ell) \subseteq \mathrm{SL}_2(F)$. The corresponding $F[Q_8]$-module W is absolutely simple and symplectic. By Schur's Lemma, every Q_8-invariant bilinear form on W is alternating. Since $\bar{\rho}_1 \oplus \bar{\rho}_1$ and the restriction of $\bar{\rho}$ to Q_8 give rise to the same characteristic polynomials, the semisimple $F[Q_8]$-modules V_0 and $W \oplus W$ are isomorphic. Since $\mathrm{End}_{Q_8}(W) = F$, we have $\mathrm{End}_{Q_8}(V_0) = M_2(F)$. Fix a generator c of $\boldsymbol{\mu}_\ell$. Then c is an element of $\mathrm{End}_{Q_8}(V_0)$ of multiplicative order ℓ. We can therefore identify V_0 with $W \oplus W$ in such a way that $c(x,y) = (x+y, y)$ for every $(x,y) \in W \oplus W = V_0$. As in the proof of Lemma 6, for $x, y \in W$ we have

$$f_0((x,0),(0,y)) = f_0(c(x,0), c(0,y)) = f_0((x,0),(y,y)) =$$

$$f_0((x,0),(0,y)) + f_0((x,0),(y,0)).$$

Therefore,

$$f_0((x,0),(y,0)) = 0 \text{ for all } x, y \in W. \tag{1}$$

Further,

$$f_0((0,x),(0,y)) = f_0(c(0,x), c(0,y)) = f_0((x,x),(y,y)) =$$

$$f_0((0,x),(0,y)) + f_0((x,0),(y,0)) + f_0((x,0),(0,y)) + f_0((0,x),(y,0)).$$

Therefore, $f_0((x,0),(0,y)) + f_0((0,x),(y,0)) = 0$. Since f_0 is alternating,

$$f_0((x,0),(0,y)) = -f_0((0,x),(y,0)) = f_0((y,0),(0,x)). \tag{2}$$

Define $h : W \times W \to F$ by $h(x,y) = f_0((x,0),(0,y))$. By (2), h is symmetric. Since f_0 is Q_8-invariant, so is h. The nondegeneracy of h follows from (1) and the nondegeneracy of f_0. Since h is a Q_8-invariant pairing on W, it is alternating. Since h is both alternating and symmetric we have $h = 0$, giving a contradiction. □

References

[1] J-P. Serre, *Exemples de plongements des groupes* $\mathrm{PSL}_2(\mathbf{F}_p)$ *dans des groupes de Lie simples*, Invent. Math. **124** (1996), 525–562.

[2] A. Silverberg, Yu. G. Zarhin, *Variations on a theme of Minkowski and Serre*, J. Pure and Applied Algebra **111** (1996), 285–302.

[3] A. Silverberg, Yu. G. Zarhin, *Symplectic representations of inertia groups*, preprint.

Department of Mathematics, Ohio State University, Columbus, Ohio 43210, USA
E-mail address: `silver@math.ohio-state.edu`

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
E-mail address: `zarhin@math.psu.edu`